



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|------------------------------|------------------------|
| 09/700,656 | 02/14/2001 | Harald Vater | JEK/VATER | 7577 |
| 7590 08/31/2009 | | | | |
| Bacon & Thomas Fourth Floor 625 Slaters Lane Alexandria, VA 22314-1176 | | | EXAMINER DAVIS, ZACHARY A | |
| | | | ART UNIT 2437 | PAPER NUMBER |
| | | | MAIL DATE 08/31/2009 | DELIVERY MODE PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/700,656

Applicant(s)

VATER ET AL.

Examiner

Zachary A. Davis

Art Unit

2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 May 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-43 is/are pending in the application.
- 4a) Of the above claim(s) 1-25, 34-41 and 43 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 26-33 and 42 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/C)
- Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-43 are currently pending in the present application. Claims 1-25, 34-41, and 43 were previously withdrawn from further consideration as being directed to nonelected inventions. Claims 26-33 and 42 are currently under consideration in the present application.

Response to Arguments

2. In view of the appeal brief filed on 14 May 2009, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 26-33 and 42 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 26-33 and 42 are directed to methods as recited. While the claims recite a series of steps or acts to be performed, a statutory process under 35 U.S.C. 101 must (1) be tied to a particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See *In re Bilski*, 545 F3d 943, 88 USPQ2d 1385, 1391 (Fed. Cir. 2008). The methods of Claims 26-33 and 42, and particularly independent Claim 26, generally include steps of “falsifying input data” and combining output data “to compensate for the falsification”. These steps only describe calculations being performed and do not clearly require any particular machine to be performed, nor is any transformation of an underlying article or material clearly apparent. It is further noted that the recitation of “a memory of a data carrier” in dependent Claim 28, while appearing to be directed to a particular machine, only relates

to insignificant extra-solution activity, namely the storage of data, and therefore, the presence of the memory of the data carrier is not sufficient to clearly limit Claim 28 to a statutory process. Therefore, the claims are not directed to statutory subject matter.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 26-33 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al, US Patent Application Publication 2002/0124178, in view of Cordery et al, US Patent 5655023.

In reference to Claim 26, Kocher discloses a method of protecting secret data, where the method includes falsifying input data by combination with auxiliary data before execution of one or more operations (paragraphs 0068, 0070, and 0072, where blinding occurs before permutation operations), and combining the output data with an auxiliary function value in order to compensate for the falsification of the input data (paragraphs paragraphs 0070, 0072, and 0073, where unblinding occurs to compensate for the blinding), where the auxiliary value was determined by executing the operations using the auxiliary data as input data (paragraph 0072, where the output buffer is initialized with the blinding bit and the data in the output buffer is the result of using the

input permutation table, i.e. the operations). However, while Kocher discloses previously determining the auxiliary data and/or values (see paragraph 0072), Kocher does not explicitly disclose determining the auxiliary value previously and in safe surroundings.

Cordery discloses a method in which secret function values are pre-computed in safe surroundings and where the secret values are maintained securely (see column 3, lines 18-25, where tokens are pre-computed, see also column 5, lines 10-12, where tokens include encrypted data, and column 3, lines 11-13, where the encryption algorithm and keys are protected; see also column 4, lines 52-59, where the tokens are stored on smart cards and protected against tampering, i.e. maintained securely). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Kocher to include pre-computation and safe storage of secret function values in order to protect the encryption algorithm and secret key used (see Cordery, column 3, lines 11-13).

In reference to Claim 27, Kocher and Cordery further disclose that the combination with the auxiliary function value is performed before execution of a non-linear operation (see Kocher, paragraph 0074, where inputs can be maintained in a blinded state and only reconstituted when nonlinear operations must be performed).

In reference to Claim 28, Kocher and Cordery further disclose that the auxiliary data are varied and function values are stored in the memory of a data carrier (Kocher, paragraphs 0072-0075; Cordery, column 4, lines 54-58).

In reference to Claims 29-32, Kocher and Cordery further disclose that new auxiliary values can be generated by combining existing values, that auxiliary data are selected randomly, pairs of auxiliary data and auxiliary function values are generated, and the auxiliary data are random numbers (see Kocher, paragraphs 0072 and 0075).

In reference to Claim 33, Kocher and Cordery further disclose combining the output data and auxiliary function value using an XOR operation (see Kocher, paragraph 0073).

In reference to Claim 42, Kocher and Cordery further disclose that operations include permutations of data (see Kocher, paragraphs 0068 and 0070-0074).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Micali et al, US Patent 5016274 and European Publication 368596, disclose systems for digital signatures that includes pre-computation of data.
- b. Kocher et al, US Patents 6304658 and 7506165, disclose systems in which various random numbers and secret values are pre-computed.
- c. Drexler et al, US Patent 7447913, discloses a method for protecting secret data, granted to the named inventors of the present application.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437